CLAIMS

1. (Currently Amended) A method comprising:

receiving a policy at a client from a host, the policy including a number of assertions for the client to comply with in order to access one or more resources via the host, wherein the policy is cached at the client, and wherein the client is configured to generate policy digests;

determining, at the client, that the client is complying with at least one assertion;

generating a policy digest at the client for the cached policy <u>by reading each of the at least one assertions from the policy, assigning a respective bit value to each of the at least one assertions, and writing each respective bit value to a bit vector</u>, the policy digest identifying the at least one assertion; and

sending a message from the client to the host to access a resource via the host, the message including the policy digest.

2. (Original) The method of claim 1, wherein generating the policy digest includes generating a hash of the cached policy.

3. (Currently Amended) The method of claim 1, wherein generating the policy digest includes encoding [[a]] <u>the</u> bit vector<u>, the bit vector</u> identifying selected assertions from the cached policy.

4. (Canceled)

5. (Original) The method of claim 1, wherein generating the policy digest includes generating a hash of the cached policy if the cached policy is normalized.

6. (Previously Presented) The method of claim 1, further comprising:

incrementing a counter at the client each time the cached policy is used; and

removing the cached policy from a cache at the client when the counter exceeds a limit value.

7. (Previously Presented) The method of claim 1, further comprising:

incrementing a counter at the client for the cached policy when a fault is received at the client in response to using the cached policy; and

removing the cached policy from a cache at the client when the counter exceeds a limit value.

8. (Previously Presented) The method of claim 1, further comprising logging a diagnostic event at the client when a fault is received at the client to identify a system problem.

9. (Currently Amended) A method comprising:

sending a policy from a host to a client, the policy including a number of assertions for the client to comply with in order to access one or more resources via the host, and wherein the host is configured to implement a host messaging module;

extracting a policy digest from a message received at the host from the client, the policy digest indicating that the client is complying with at least one assertion of the number of assertions of the policy in order to access the one or more resources via the host and the policy digest including a bit vector identifying the at least one assertion;

returning, by the host, an invalid digest fault to the client when a length of the bit vector is not valid; and

determining, by the host, whether the at least one assertion is valid when the length of the bit vector is valid

~~determining, at the host, whether the policy is valid; and~~

~~denying access to the resource at the host if the policy digest identifies an invalid policy.~~

10. (Previously Presented) The method of claim 9, further comprising issuing a fault at the host for the client if the policy digest identifies an invalid policy.

11. (Previously Presented) The method of claim 9, further comprising decoding the policy digest at the host.

12. (Currently Amended) The method of claim 9, further comprising decoding [[a]] the bit vector ~~of the policy~~ at the host.

13. (Previously Presented) The method of claim 9, further comprising reading an assertion from the policy digest at the host.

14. (Previously Presented) The method of claim 9, further comprising reading a row hash of the policy at the host.

15. (Previously Presented) A system comprising:

a processing unit; and

a system memory accessible to the processing unit, the system memory including:

a message processor to:

receive a message from a client to access a resource; and

extract a policy digest from the message, the policy digest indicating that the client is complying with one or more of a number of assertions of a policy in order to access one or more resources via the system and the policy digest including a bit vector identifying the one or more assertions; and

a fault generator to:

return an invalid digest fault to the client when a length of the bit vector is not valid; and

determine whether the one or more assertions are valid when the length of the bit vector is valid.

16. (Canceled)

17. (Previously Presented) The system of claim 15, wherein the message processor is configured to decode the policy digest.

18. (Previously Presented) The system of claim 15, wherein the fault generator is configured to return an invalid policy fault to the client when at least one of the one or more assertions specified in the policy digest is invalid.

19. (Original) The system of claim 15, wherein the policy digest is a row hash of a normalized policy.

20. (Original) The system of claim 15, wherein the policy digest identifies at least one selected assertion.

21. (Previously Presented) A system comprising:

a processor; and

a memory accessible to the processor, the memory including:

a digest generator to:

generate a policy digest based on one or more policies received at a client from a host, the one or more policies each specifying at least one assertion that the client must comply with in order to access a resource via the host; and

place a bit vector in a header of a message to access a particular resource of the host, the bit vector including one bit for each assertion of a particular policy and including one bit for each assertion of an additional policy referenced by the particular policy.

22. (Previously Presented) The system of claim 21, further comprising a messaging module to encode the policy digest.

23. (Previously Presented) The system of claim 21, further comprising a cache including the one or more policies.

24. (Original) The system of claim 21, wherein the policy digest is a row hash of a normalized policy.

25. (Original) The system of claim 21, wherein the policy digest identifies at least one assertion selected by the client.

26. (Previously Presented) One or more computer-readable storage media encoding a computer program for executing on a computer system a computer process, the computer process comprising:

receiving a policy at a client from a host, the policy including a number of assertions for the client to comply with in order to access one or more resources via the host, and wherein the policy is cached at the client;

determining, at the client, that the client is complying with at least one assertion;

generating a policy digest at the client for the cached policy, the policy digest identifying the at least one assertion the client is complying with;

sending a message from the client to the host, the message including a request to access a particular resource via the host and the message including the policy digest;

receiving a fault at the client from the host, the fault indicating that the policy is invalid;

removing the policy from a cache at the client in response to receiving the fault; and

sending a request from the client to the host for a valid policy after removing the policy from the cache.

27. (Previously Presented) The one or more computer-readable storage media of claim 26 wherein the computer process further comprises generating a hash of the cached policy.

28. (Previously Presented) The one or more computer-readable storage media of claim 26 wherein the computer process further comprises encoding a bit vector of the cached policy.

29. (Previously Presented) The one or more computer-readable storage media of claim 26 wherein the computer process further comprises reading an assertion from the policy, assigning a bit value to the assertion, and writing the bit value to a bit vector.

30. (Previously Presented) The one or more computer-readable storage media of claim 26 wherein the computer process further comprises generating a row hash of the cached policy if the cached policy is normalized.

31. (Previously Presented) The one or more computer-readable storage media of claim 26, wherein the computer process further comprises:

incrementing a counter each time the cached policy is used; and

removing the cached policy from a cache at the client when the counter exceeds a limit value.

32. (Previously Presented) The one or more computer-readable storage media of claim 26 wherein the computer process further comprises:

incrementing a counter for the cached policy when the fault is received at the client in response to using the cached policy; and

removing the cached policy from the cache at the client when the counter exceeds a limit value.

33. (Previously Presented) The one or more computer-readable storage media of claim 26 wherein the computer process further comprises triggering a diagnostic event when the fault is received at the client.

34. (Currently Amended) One or more computer-readable storage media encoding a computer program for executing on a computer system a computer process, the computer process comprising:

extracting at a host a policy digest included in a message from a client, the policy digest indicating that the client is complying with an assertion required to access a resource via the host, ~~and~~ the assertion is associated with a policy, and the policy digest includes a bit vector identifying the assertion;

returning, by the host, an invalid digest fault to the client when a length of the bit vector is not valid; and

determining, by the host, whether the assertion is valid when the length of the bit vector is valid

~~denying access to the resource at the host if the policy digest identifies an invalid policy~~.

35. (Previously Presented) The one or more computer-readable storage media of claim 34 wherein the computer process further comprises decoding the policy digest.

36. (Currently Amended) The one or more computer-readable storage media of claim 34 wherein the computer process further comprises decoding [[a]] <u>the</u> bit vector ~~of the policy~~.

37. (Previously Presented) The one or more computer-readable storage media of claim 34 wherein the computer process further comprises reading the assertion from the policy digest.

38. (Previously Presented) The one or more computer-readable storage media of claim 34 wherein the computer process further comprises reading a row hash of the policy if the policy is normalized.